

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06162289 A**

(43) Date of publication of application: **10 . 06 . 94**

(51) Int. Cl

**G06K 19/10  
G06F 15/21  
G06K 17/00  
G09C 1/00**

(21) Application number: **04308688**

(22) Date of filing: **18 . 11 . 92**

(71) Applicant:

**NIPPON TELEGR & TELEPH CORP <NTT>**

(72) Inventor:

**ISHIGURO GINYA  
MUTA TOSHIYASU  
SAKIDA KAZUTAKA**

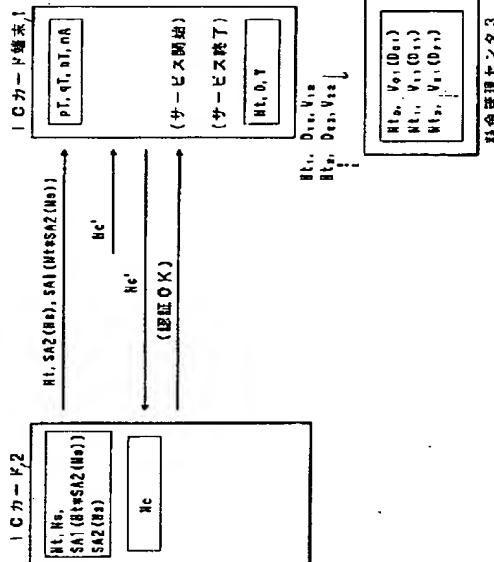
**(54) IC CREDIT CARD AND IC CARD TERMINAL**

(57) Abstract:

PURPOSE: To dispense with the check of the legality of an user by a center at the time of receiving service.

CONSTITUTION: At the time of issuing an IC card 2, a registration number Nt assigned at every user, a set number Ns for setting a password number use, a digital signature SA2 (Ns) prepared by the master key of an issuer and the digital signature SA1{Nt\*SA1(Ns)} prepared by the master key with SA2 (Ns) and Nt are stored in the EEPROM of the IC card 2. At the time of registering the password number Nc, the legality of the user is checked and verified with the IC card 2 by communication with an IC card terminal 1 by Ns known only to the user. By inserting the IC card 2, Nt, SA2 and SA1 are transmitted to the terminal 1 and the terminal 1 verifies SA1 by an open key nA, checks the legality of Nt and when it is correct, let the password number be inputted. When the user inputs Nc', the IC card 2 compares it with Nc of the inside and transmits authentication to the terminal 1 in the case of coincidence and when it is received, the terminal 1 permits the user to receive the service.

COPYRIGHT: (C)1994,JPO&Japio



Best Available Copy

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-162289

(43)公開日 平成6年(1994)6月10日

(51)Int.Cl.<sup>5</sup>  
G 0 6 K 19/10  
G 0 6 F 15/21  
G 0 6 K 17/00  
G 0 9 C 1/00

識別記号 340 B 7052-5L  
T 7459-5L  
8837-5L  
8623-5L

F I

技術表示箇所

G 0 6 K 19/00

R

審査請求 未請求 請求項の数2(全10頁)

(21)出願番号 特願平4-308688

(22)出願日 平成4年(1992)11月18日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72)発明者 石黒 銀矢

東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

(72)発明者 牟田 敏保

東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

(72)発明者 崎田 一貴

東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

(74)代理人 弁理士 草野 卓

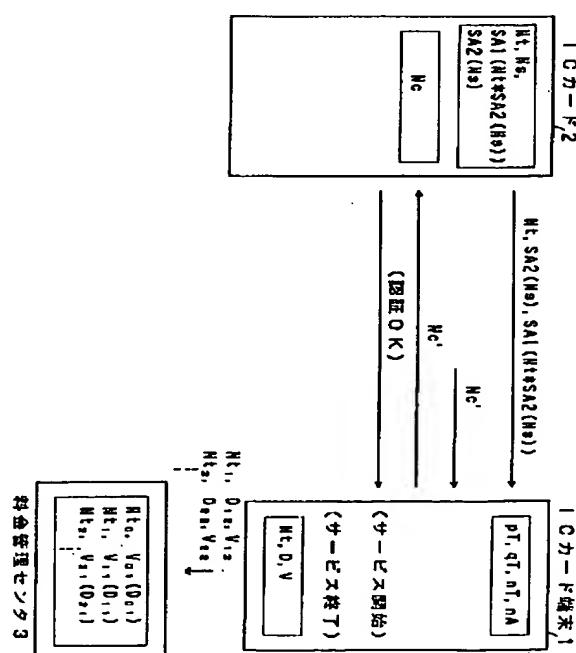
(54)【発明の名称】 ICクレジットカード及びICカード端末

(57)【要約】 (修正有)

【目的】 サービスを受けるに当たりセンタによる利用者の正当性のチェックの不要化。

【構成】 ICカード2発行の際、利用者ごとに割付けられた登録番号N<sub>t</sub>と、暗証番号設定用設定番号N<sub>s</sub>と、発行者のマスタ鍵でN<sub>s</sub>に作成したデジタル署名S<sub>A2</sub>(N<sub>s</sub>)と、S<sub>A2</sub>(N<sub>s</sub>)とN<sub>t</sub>にマスタ鍵で作成したデジタル署名S<sub>A1</sub>(N<sub>t</sub>\*S<sub>A1</sub>(N<sub>s</sub>))とをICカード2のEEPROMに記憶しておく。暗証番号N<sub>c</sub>登録の際は、利用者しか知らないN<sub>s</sub>で利用者の正当性をICカード端末1とのやりとりでICカード2でチェック検証する。ICカード2の挿入で、N<sub>t</sub>、S<sub>A2</sub>、S<sub>A1</sub>が端末1へ送られ、端末1は公開鍵n<sub>A</sub>でS<sub>A1</sub>を検証し、N<sub>t</sub>の正当性をチェックし、正しければ暗証番号を入力させる。利用者のN<sub>c'</sub>入力で、ICカード2は内部のN<sub>c</sub>と比較し、一致すれば認証化を端末1へ送り端末1はこれを受けると利用者にサービスを受けることを許す。

図5



**【特許請求の範囲】**

**【請求項1】** 利用者を特定するための登録番号N<sub>t</sub>、暗証番号を設定するための設定番号N<sub>s</sub>、前記登録番号N<sub>t</sub>を含む情報に対するマスタ鍵によるデジタル署名S<sub>A</sub>を記録するとともに、暗証番号N<sub>c</sub>を記録するためのメモリと、前記登録番号N<sub>t</sub>、前記デジタル署名S<sub>A</sub>をICカード端末へ送信する手段と、

前記ICカード端末から受信した設定番号N<sub>s'</sub>と前記メモリに記録している設定番号N<sub>s</sub>との比較を行い、一致したとき第1の認証通知を前記ICカード端末へ送信する手段と、暗証番号登録時に、前記ICカード端末から暗証番号N<sub>c</sub>、その暗証番号N<sub>c</sub>を含む情報に対する前記ICカード端末によるデジタル署名S<sub>T</sub>、前記ICカード端末の端末公開鍵n<sub>T</sub>を受信し、前記受信したデジタル署名S<sub>T</sub>を受信した端末公開鍵n<sub>T</sub>で検証し、正しい場合にのみ前記メモリに受信した暗証番号N<sub>c</sub>を記録する手段と、

サービス開始前に、前記ICカード端末から受信した暗証番号N<sub>c'</sub>と前記メモリに記録している暗証番号N<sub>c</sub>との比較を行い、一致したとき第2の認証通知を前記ICカード端末へ送信する手段と、を具備するICクレジットカード。

**【請求項2】** デジタル署名S<sub>A</sub>を検証するためのマスタ公開鍵n<sub>A</sub>及び端末公開鍵n<sub>T</sub>、デジタル署名をするための端末鍵p<sub>T</sub>、q<sub>T</sub>を記録したメモリと、

ICカードから受信したデジタル署名S<sub>A</sub>を前記公開鍵n<sub>A</sub>で検証し、受信した登録番号N<sub>t</sub>が正しければ暗証番号の登録または暗証番号の入力を許可する手段と、暗証番号の登録が選択されたとき、入力手段から入力された登録番号N<sub>t'</sub>と受信した登録番号N<sub>t</sub>との比較を行い、一致したとき設定番号の入力を指示する手段と、前記入力手段から入力された設定番号N<sub>s'</sub>を前記ICカードへ送信する手段と、

前記ICカードから第1の認証通知を受信したとき、前記入力手段から入力された暗証番号N<sub>c</sub>を含む情報に対して前記端末鍵p<sub>T</sub>、q<sub>T</sub>を用いてデジタル署名S<sub>T</sub>を作成する手段と、

前記暗証番号N<sub>c</sub>、前記デジタル署名S<sub>T</sub>、前記端末公開鍵n<sub>T</sub>を前記ICカードに送信する手段と、

暗証番号の入力が選択されたとき、前記入力手段から入力された暗証番号N<sub>c'</sub>を前記ICカードに送信する手段と、

前記ICカードから第2の認証通知を受信したとき、サービスを許可する手段と、

を具備したICカード端末。

**【発明の詳細な説明】**

**【0001】**

**【産業上の利用分野】** この発明は、あらかじめ登録番号

などを登録してあるICカードをICカード端末へ利用者が挿入することによりサービスの提供を受け、そのサービスについて後に料金の請求を受けるようにしたICクレジットカードシステムに用いられる前記ICクレジットカード及び前記ICカード端末に関する。

**【0002】**

**【従来の技術】** 従来のICクレジットカードシステムは、サービス提供前に、ICカード端末と、登録番号などを登録しているセンタとをオンラインでつなぎ、利用者がダイヤル操作により登録番号などを入力し、入力された情報がセンタに送られ、センタであらかじめ登録されている利用者情報により利用者の正当性のチェックが行われ、正当であることが確認されたとき、ICカード端末でのサービスの提供を可能としていた。

**【0003】**

**【発明が解決しようとする課題】** したがって、従来においては、サービス提供前にセンタとICカード端末とが通信を行う必要があり、オンラインで検証を行うためにセンタ設備が大規模になったり、通信料がサービス提供料金の他に必要になるなど欠点があった。

**【0004】**

**【課題を解決するための手段】** この発明によるICクレジットカードは、利用者を特定するための登録番号N<sub>t</sub>、暗証番号を設定するための設定番号N<sub>s</sub>、前記登録番号N<sub>t</sub>を含む情報に対するマスタ鍵によるデジタル署名S<sub>A</sub>を記録するとともに、暗証番号N<sub>c</sub>を記録するためのメモリと、前記登録番号N<sub>t</sub>、前記デジタル署名S<sub>A</sub>をICカード端末へ送信する手段と、前記ICカード端末から受信した設定番号N<sub>s'</sub>と前記メモリに記録している設定番号N<sub>s</sub>との比較を行い、一致したとき第1の認証通知を前記ICカード端末へ送信する手段と、暗証番号登録時に、前記ICカード端末から暗証番号N<sub>c</sub>、前記暗証番号を含む情報に対する前記ICカード端末によるデジタル署名S<sub>T</sub>、前記ICカード端末の端末公開鍵n<sub>T</sub>を受信し、その受信したデジタル署名S<sub>T</sub>を前記端末公開鍵n<sub>T</sub>で検証し、正しい場合にのみ前記メモリに受信した暗証番号N<sub>c</sub>を記録する手段と、サービス開始前に、前記ICカード端末から受信した暗証番号N<sub>c'</sub>と前記メモリに記録している暗証番号N<sub>c</sub>との比較を行い、一致したとき第2の認証通知を前記ICカード端末へ送信する手段とを具備する。

**【0005】** この発明によるICカード端末は、デジタル署名S<sub>A</sub>を検証するためのマスタ公開鍵n<sub>A</sub>及び端末公開鍵n<sub>T</sub>、デジタル署名をするための端末鍵p<sub>T</sub>、q<sub>T</sub>を記録したメモリと、受信したデジタル署名S<sub>A</sub>を前記公開鍵n<sub>A</sub>で検証し、受信した登録番号N<sub>t</sub>が正しければ暗証番号の登録または暗証番号の入力を許可する手段と、暗証番号の登録が選択されたとき、入力手段から入力された登録番号N<sub>t'</sub>と受信した登録番号N<sub>t</sub>との比較を行い、一致したとき設定番号の入力を指示する手

段と、入力手段から入力された設定番号N s' を I C カードへ送信する手段と、前記 I C カードから第 1 の認証通知を受信したとき、入力手段から入力された暗証番号 N c を含む情報に対して前記端末鍵 p T、q T を用いてデジタル署名 S T を作成する手段と、前記暗証番号 N c、前記デジタル署名 S T、前記端末公開鍵 n T を前記 I C カードに送信する手段と、暗証番号の入力が選択されたとき、入力手段から入力された暗証番号 N c' を前記 I C カードに送信する手段と、前記 I C カードから第 2 の認証通知を受信したとき、サービスを許可する手段とを具備する。

#### 【0006】

【作用】このような構成の I C クレジットカード（以下単に I C カードと記す）、I C カード端末を設ければ、デジタル署名付きの登録番号によって I C カードの正当性を I C カード端末で検証できるとともに、利用者が入力した暗証番号により、利用者の正当性を I C カードで検証でき、さらに暗証番号の登録時には利用者しか知り得ない設定番号により利用者の正当性を I C カードで検証できるので利用者の情報に関するデータベースを持つセンタへサービス開始前にアクセスする必要がなく、しかも不正な I C カードによるサービス利用も排除することができる。

#### 【0007】

【実施例】次に図を参照にして請求項 1 及び 2 の発明の各実施例を説明する。図 1 は、この発明の I C カード及び I C カード端末が適用される I C クレジットカードシステム構成例を示す。I C カード端末 1 は I C カード 2 により検証処理を行い、通話など各種サービスを提供する。料金管理センタ 3 は I C カード 2 により利用したサービス料金を管理する。I C カード端末 1 は利用された I C カード 2 の登録番号と利用料金をメモリに蓄えておき、適当な間隔、例えば日ごとに料金管理センタ 3 へ自動的に発信し、蓄えた情報を料金管理センタ 3 へ通信網 4 を介して送信する。料金管理センタ 3 では登録番号ごとに利用料金を集計し、例えば月ごとに利用者へ利用料金の請求を行う。

【0008】図 2 は I C カード端末 1 の内部構成を示す図であり、制御部 11 は処理手順などのプログラムを内部の ROM に記録しているとともに、鍵情報などを内部 RAM に記録している。鍵情報などは、I C カード端末設置時に、通信網を介してセンタ装置（図示せず）と接続し、センタ装置から受信して RAM に記録してもよく、I C カード端末製造時に予め設定してもよい。I C カード 2 とデータのやりとりを行う I C カードリーダライタ部 12、暗証番号の登録を指示する操作ボタン、ダイヤルボタンなどからなる操作入力部 13、液晶ディスプレイからなる表示部 14 及び通話回路 15 が制御部 11 に接続され、通話回路 15 に送受器 16 が接続された通信網との処理を行う通信処理部 17 が制御部 11 に

接続されている。

【0009】図 3 は I C カード 2 の内部構成を示す図であり、I C カードの処理手順等のプログラムは ROM 6 1 に記憶され、CPU 6 3 はワークエリアとして RAM 6 2 を利用してすべての制御を行い、図 2 に示した I C カード端末 1 の I C カードリーダライタ部 12 との通信は通信部 6 5 により接点 6 6 を介して行われる。登録番号、設定番号、デジタル署名は I C カード 2 の発行時に I C カード発行機（図示せず）によって書き込まれ EEPROM 6 4 に記録されている。

【0010】図 4 は利用者が I C カード端末 1 を使って I C カード 2 に暗証番号を登録する操作を説明する図である。I C カード 2 の EEPROM 6 4 の所定エリアに、利用者を特定するための登録番号 N t、暗証番号を設定するために利用者ごとに割り付けられた設定番号 N s、その設定番号 N s に対して発行者がマスタ鍵によって作成した第 2 のデジタル署名 SA 2 (N s)、登録番号 N t および第 2 のデジタル署名 SA 2 (N s) に対して発行者がマスタ鍵によって作成した第 1 のデジタル署名 SA 1 (N t \* SA 2 (N s)) が記録されている。

この記録の際に第 2 のデジタル署名 SA 2 (N s) を公開鍵 n A で検証して設定番号 N s の正当性を判断することができる。また、I C カード端末 1 の制御部 11 内の RAM の所定のエリアに、前記マスタ鍵によって作成されたデジタル署名を検証するためのマスタ公開鍵 n A、I C カードが端末がデジタル署名を作成するための端末鍵 p T、q T、前記 I C カード端末が作成したデジタル署名を検証するための端末公開鍵 n T が記録されている。デジタル署名としては、例えば「NTT R&D Vo 1.40 No.5 P. 687~696 (1991)」に掲載されている E S IGN を使用することができる。

【0011】利用者が I C カード 2 を I C カード端末 1 の I C カードリーダライタ部 12 に挿入すると、I C カード 2 から I C カード端末 1 に登録番号 N t、第 2 のデジタル署名 SA 2 (N s)、第 1 のデジタル署名 SA 1 (N t \* SA 2 (N s)) が送信される。I C カード端末 1 はマスタ公開鍵 n A により第 1 のデジタル署名 SA 1 の検証を行い、N t の正当性を判断する。この場合第 2 のデジタル署名 SA 2 の検証も行い、これの正当性も判断すると一そう正確になる。正当でないと判断した場合には I C カードを返却して処理を中止する。両者とも正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部 14 に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部 13 のボタン操作による暗証番号の登録を有効とする。ここで、暗証番号を入力しても I C カード 2 に暗証番号が登録されなければ暗証番号不一致として処理される。操作入力部 13 の暗証番号登録ボタンを押すことにより暗証番号登録処理に移行する。I C カー

ド 2 へ暗証番号登録通知を送信し、I C カード 2 へ暗証

番号登録処理に入ったことを知らせるとともに、表示部14に“登録番号をダイヤルしてください”と表示し、利用者に登録番号の入力を促す。利用者がダイヤルにより登録番号N<sub>t'</sub>を入力すると、ICカード端末1は先にICカード2から受信した登録番号N<sub>t</sub>との比較を行い、利用者が入力した番号の正当性をチェックする。一致しない場合には再度登録番号の入力を促すが、例えば3回の入力後も一致しない場合には、不正使用と判断しICカード2を返却して処理を中止する。一致した場合には表示部14に“設定番号をダイヤルしてください”と表示し、利用者に設定番号の入力を促す。

【0012】利用者がダイヤルにより設定番号N<sub>s'</sub>を入力すると、ICカード端末1はICカード2へ設定番号N<sub>s'</sub>を送信する。ICカード2は受信した設定番号N<sub>s'</sub>と前記メモリに予め記録している設定番号N<sub>s</sub>との比較を行い、利用者が入力した設定番号の正当性をチェックする。一致しない場合にはICカード端末1へ不一致通知を送信し、ICカード端末1は再度設定番号の入力を促すが、例えば3回の入力後も一致しない場合には、不正使用と判断しICカード2を返却して処理を中止する。一致した場合にはICカード2は認証OK(第1の認証通知)をICカード端末1へ送信する。ICカード端末1は表示部14に“暗証番号をダイヤルしてください”と表示し、利用者に暗証番号の入力を促す。利用者がダイヤルにより暗証番号N<sub>c</sub>を入力すると、ICカード端末1は暗証番号N<sub>c</sub>に対して端末鍵p<sub>T</sub>、q<sub>T</sub>によるデジタル署名ST(N<sub>c</sub>)を作成し、ICカード2に暗証番号N<sub>c</sub>とともにデジタル署名ST(N<sub>c</sub>)および端末公開鍵n<sub>T</sub>を送信する。ICカード2は端末公開鍵n<sub>T</sub>によりデジタル署名ST(N<sub>c</sub>)の検証を行い、暗証番号N<sub>c</sub>の正当性のチェックを行う。正当であることが検証できた場合には暗証番号N<sub>c</sub>をRAM62に記録する。

【0013】上記の処理において、設定番号N<sub>s</sub>の検証をICカード2で行うようにしているが、最初に登録番号N<sub>t</sub>をICカード端末1へ送信するときに設定番号N<sub>s</sub>もいっしょに送信しておけばICカード端末1で設定番号のチェックを行うことができる。ただし、この場合には設定番号N<sub>s</sub>という他人には知られてはならない情報がICカード2から送信されるためセキュリティという面からは好ましくない。また、登録番号あるいは設定番号のダイヤル時に、3回の入力後も一致しない場合には、不正カードである旨をICカード2に記録することにより、以降そのICカードの使用を不能とすることもできる。

【0014】図5は利用者がICカード2を使ってICカード端末1からサービスを受けるときの処理を説明する図である。ICカード2のRAM62には暗証番号N<sub>c</sub>が記録されている。利用者がICカード2をICカード端末1のICカードリーダライタ部12に挿入する

と、ICカード2からICカード端末1に登録番号N<sub>t</sub>、第2のデジタル署名SA2(N<sub>s</sub>)、第1のデジタル署名SA1(N<sub>t</sub>\*SA2(N<sub>s</sub>))が送信される。ICカード端末1はマスタ公開鍵n<sub>A</sub>によりデジタル署名SA1の検証を行い、登録番号N<sub>t</sub>の正当性を判断する。この場合も第2のデジタル署名の正当性を判断した方がよい。正当でないと判断した場合にはICカード2を返却し処理を中止する。正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部14に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部13のボタン操作による暗証番号の再登録も有効である。つまり暗証番号を変更することもできる。ここで、利用者が暗証番号N<sub>c'</sub>をダイヤルすると、このN<sub>c'</sub>はICカード2へ送信され、ICカード2内でその内部に記録してある暗証番号N<sub>c</sub>との比較が行われる。一致しない場合にはICカード2からICカード端末1へ認証不一致通知が送信され、ICカード端末1は再度暗証番号の入力を促す。例えば3回の入力後も一致しない場合には、不正使用と判断してICカード2を返却して処理を中止する。

【0015】一致した場合にはICカード2は認証OK(第2の認証通知)をICカード端末1へ送信する。ICカード端末1は、所定のサービスが可能であることを表示部14に表示し、所定のサービスを実行する。例えば通常の通話サービスであれば、相手の番号がダイヤルできる旨を表示し、利用者のダイヤルした相手に接続する。これにより通話サービスを受けることができ、利用者がそのサービス利用を終了すると、ICカード端末1はその利用者を特定する登録番号N<sub>t</sub>、利用日時D、利用料金Vを内部のメモリに記録し、ICカード2を排出して処理を終了する。その内部のメモリに蓄えたデータは、例えば1日に一回程度の割合で料金管理センタ3に送信する。料金管理センタ3ではこれを受信して登録番号ごとに料金を集計し、毎月利用者に請求書を送付して料金の支払いを受ける。

【0016】図6はこの発明の他の実施例を示し、利用者がICカード端末1を使ってICカード2に暗証番号を登録する操作を説明する図である。ICカード2のEEPROM64にはN<sub>t</sub>、Ns、SA2(N<sub>s</sub>)、SA1(N<sub>t</sub>\*SA2(N<sub>s</sub>))が記録されている他に、ICカード2がデジタル署名を作成するためのカード鍵p<sub>U</sub>およびq<sub>U</sub>、ICカードが作成したデジタル署名を検証するためのカード公開鍵n<sub>U</sub>も記録されている。また、ICカード2およびICカード端末1は各々乱数生成用のプログラムをメモリに記録している。暗証番号の登録処理において、前述した手順により登録番号、設定番号の検証を終え、利用者がダイヤルボタンから暗証番号N<sub>c</sub>を入力すると、ICカード端末1は乱数Rを生成し、ICカード2へ乱数Rを送信する。ICカード2は乱数Xを生成し、受信した乱数Rおよび生成した乱数X

に対してカード鍵  $p U$ 、 $q U$  を用いてデジタル署名  $SU$  ( $R * X$ ) を作成し、作成したデジタル署名  $SU$  ( $R * X$ ) とともに乱数  $X$  およびカード公開鍵  $n U$  を IC カード端末 1 へ送信する。

【0017】IC カード端末 1 は受信したカード公開鍵  $n U$  により受信したデジタル署名  $SU$  を検証し、IC カード 2 が正当な相手であることを認証する。正当な相手であることを認証すると、乱数  $R$  および  $X$ 、暗証番号  $N c$  に対して端末鍵  $p T$ 、 $q T$  によりデジタル署名  $ST$  ( $R * X * N c$ ) を作成し、作成したデジタル署名  $ST$  ( $R * X * N c$ ) とともに端末公開鍵  $n T$ 、暗証番号  $N c$  を IC カード 2 へ送信する。IC カード 2 は受信した端末公開鍵  $n T$  によりデジタル署名  $ST$  を検証し、IC カード端末 1 が正当な相手であることを認証するとともに暗証番号の正当性を認証し、暗証番号  $N c$  を RAM 6 2 に記録する。この実施例の場合には情報の送受に相互に生成した乱数を使用しているため信号の内容が同一になることがなく、傍受した信号を利用した不正を防止することができる。また、相互にデジタル署名を作成して相互認証を行っているためセキュリティをより高めることができる。

【0018】図 7 はこの発明の他の実施例を示し、図 6 で説明した IC カード 2 および IC カード端末 1 によりサービスを受けるときの処理を説明する図である。利用者が IC カード 2 を IC カード端末 1 へ挿入し、図 5 で前述した手順により登録番号の検証を終え、利用者がダイヤルボタンから暗証番号  $N c'$  を入力すると、IC カード端末 1 は乱数  $R$  を生成し、IC カード 2 へ乱数  $R$ 、及び暗証番号  $N c'$  を送信する。IC カード 2 は受信した暗証番号  $N c'$  とメモリに記録している暗証番号  $N c$  との比較を行い、一致していれば乱数  $X$  を生成し、受信した乱数  $R$  および生成した乱数  $X$  に対してカード鍵  $p U$ 、 $q U$  によりデジタル署名  $SU$  ( $R * X$ ) を作成し、その作成したデジタル署名  $SU$  ( $R * X$ ) とともに乱数  $X$  およびカード公開鍵  $n U$  を IC カード端末 1 へ送信する。IC カード端末 1 は受信したカード公開鍵  $n U$  により受信したデジタル署名  $SU$  を検証し、IC カード 2 が正当な相手であることを認証するとともに暗証番号が正当であると判断し、所定のサービスが可能であることを表示部 1 4 に表示し、所定のサービスを実行する。サービスが終了すると、利用者を特定する登録番号  $N t$ 、利用日時  $D$ 、利用料金  $V$  を内部のメモリに記録し、IC カード 2 を排出して処理を終了する。

【0019】上記の説明において、IC カード 2 を特定するカード番号  $IDU$  と、カード番号に対して発行者がマスタ鍵により作成したデジタル署名  $SA$  ( $IDU$ ) とを IC カード 2 の発行時に EEPROM 6 4 に記録しておき、IC カード 2 を IC カード端末 1 に挿入したとき、登録番号  $N t$  とともにカード番号  $IDU$ 、デジタル署名  $SA$  ( $IDU$ ) を送信し、マスタ公開鍵によって  $S$

$A$  を検証することによりカード番号の正当性をチェックするように構成すれば、IC カード 2 の紛失などに対処することができる。すなわち、IC カード 2 を紛失したときに利用者が発行者に申告することにより、発行者は IC カード 2 のカード番号をダウンロードにより IC カード端末 1 にブラックリストとして登録する。IC カード端末 1 は IC カード 2 が挿入されたときカード番号  $IDU$  とブラックリストとを比較する。一致する IC カードがあつた場合にはその IC カードの使用を制限することができる。

【0020】また、IC カード 2 の EEPROM 6 4 に日付情報を記録しておき、IC カード 2 を IC カード端末 1 に挿入したとき、登録番号とともに日付情報を送信し、IC カード端末 1 に内蔵したカレンダーと比較することにより IC カード 2 の使用可否を判断するように構成すれば有効期限付きの IC カード 2 とすることができる。

【0021】さらに、IC カード 2 および IC カード端末 1 に送信情報の暗号化のためのアルゴリズムと暗号化および復号化のための共通の鍵をメモリに記録しておくことにより、相互の通信を暗号通信により行うことができ、よりセキュリティを高めることができる。

#### 【0022】

【発明の効果】この発明による IC カードと IC カード端末とを用いられれば、IC カードと IC カード端末との間で相互の正当性を検証することになり、かつ利用者の正当性を、IC カード端末を介して IC カードで検証するようになり、サービスの利用時あるいは暗証番号の設定時に利用者の情報に関するデータベースを持つセンタへアクセスする必要がなく、容易にシステムを構築することができる。また、センタへアクセスする必要がないため検証時間も短縮でき、操作性にすぐれたシステムとなる。さらに、発行者しか知り得ないマスタ鍵によるデジタル署名により登録番号の検証を行うように構成しているため、例え他人の登録番号を知り得てもデジタル署名を作成することはできず、また、拾った IC カードでは暗証番号が分からず、登録番号、設定番号が不明なため暗証番号を変更することも不可能でありセキュリティの高いシステムを構築することができる。

#### 【図面の簡単な説明】

【図 1】この発明の IC カード、IC カード端末を使用して IC クレジットカードシステムを構成した例を示すブロック図。

【図 2】この発明による IC カード端末の構成例を示すブロック図。

【図 3】この発明による IC カードの構成例を示すブロック図。

【図 4】この発明による IC カードと IC カード端末とを用いて、IC カードに暗証番号を登録する場合の処理手順を示す図。

【図5】図4で示した手法で登録された暗証番号のICカードによりサービスを受ける場合の処理手順を示す図。

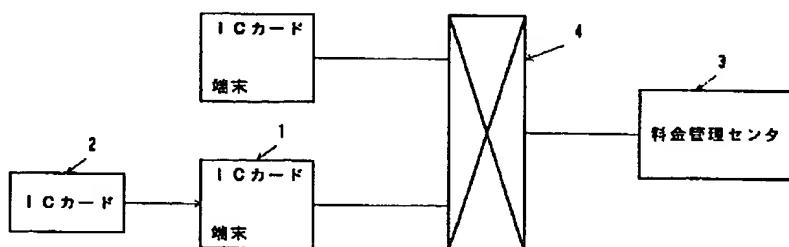
【図6】この発明の他の実施例により暗証番号を登録す\*

\*る場合の処理手順を示す図。

【図7】図6で示した手順で登録された暗証番号のICカードによりサービスを受ける場合の処理手順を示す図。

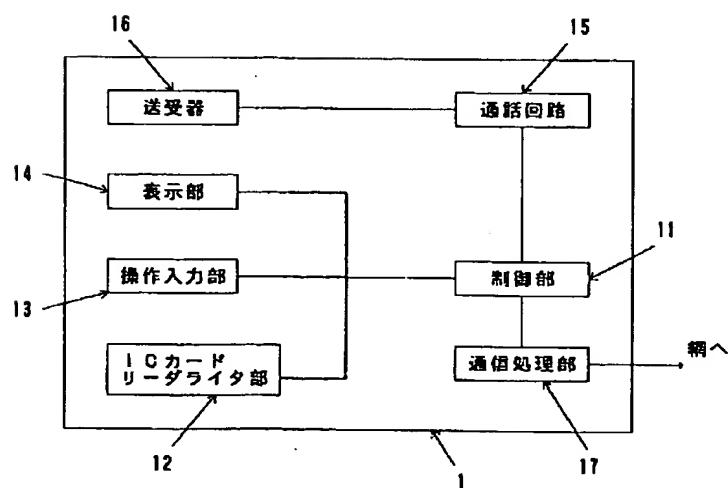
【図1】

図1



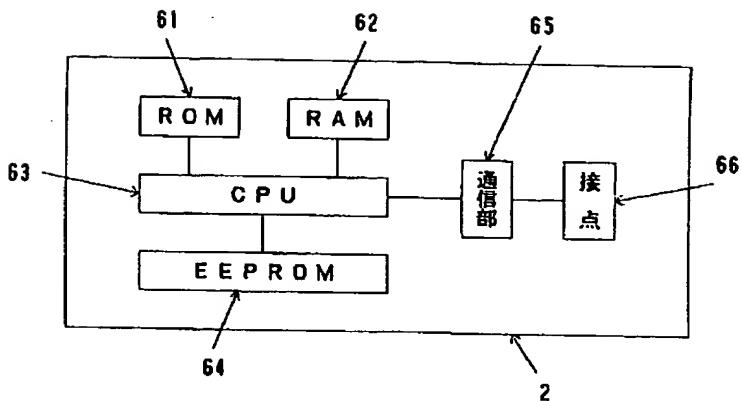
【図2】

図2



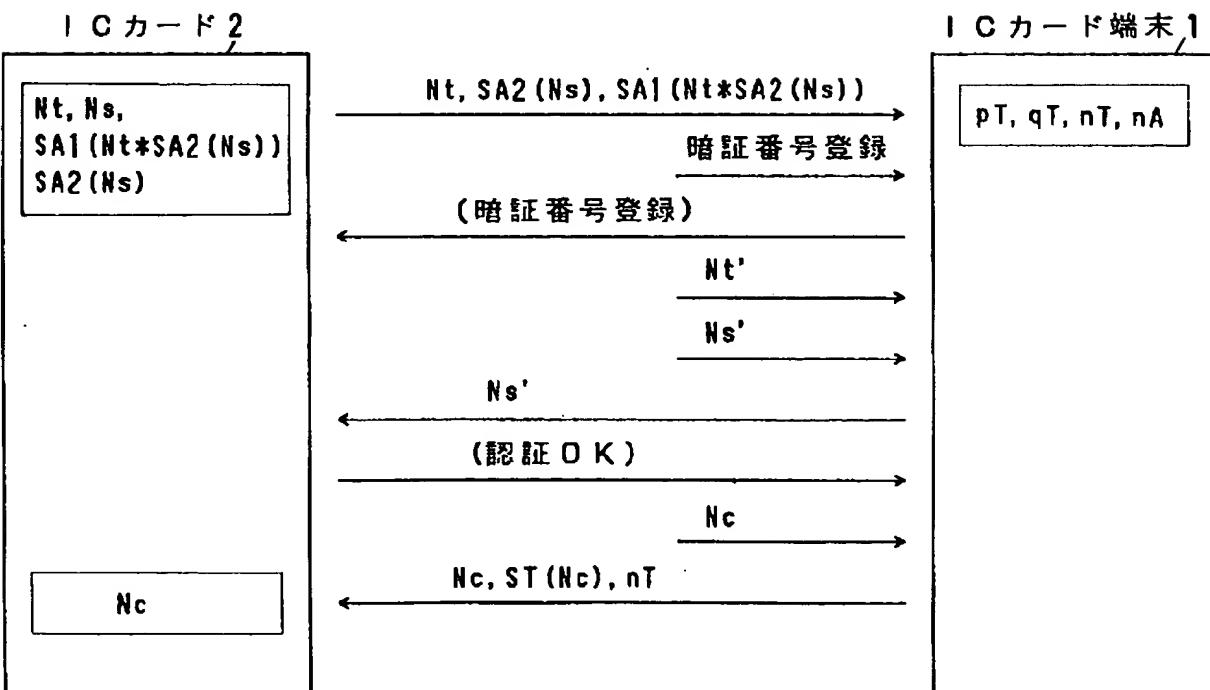
【図3】

図3



【図4】

図4



【図5】

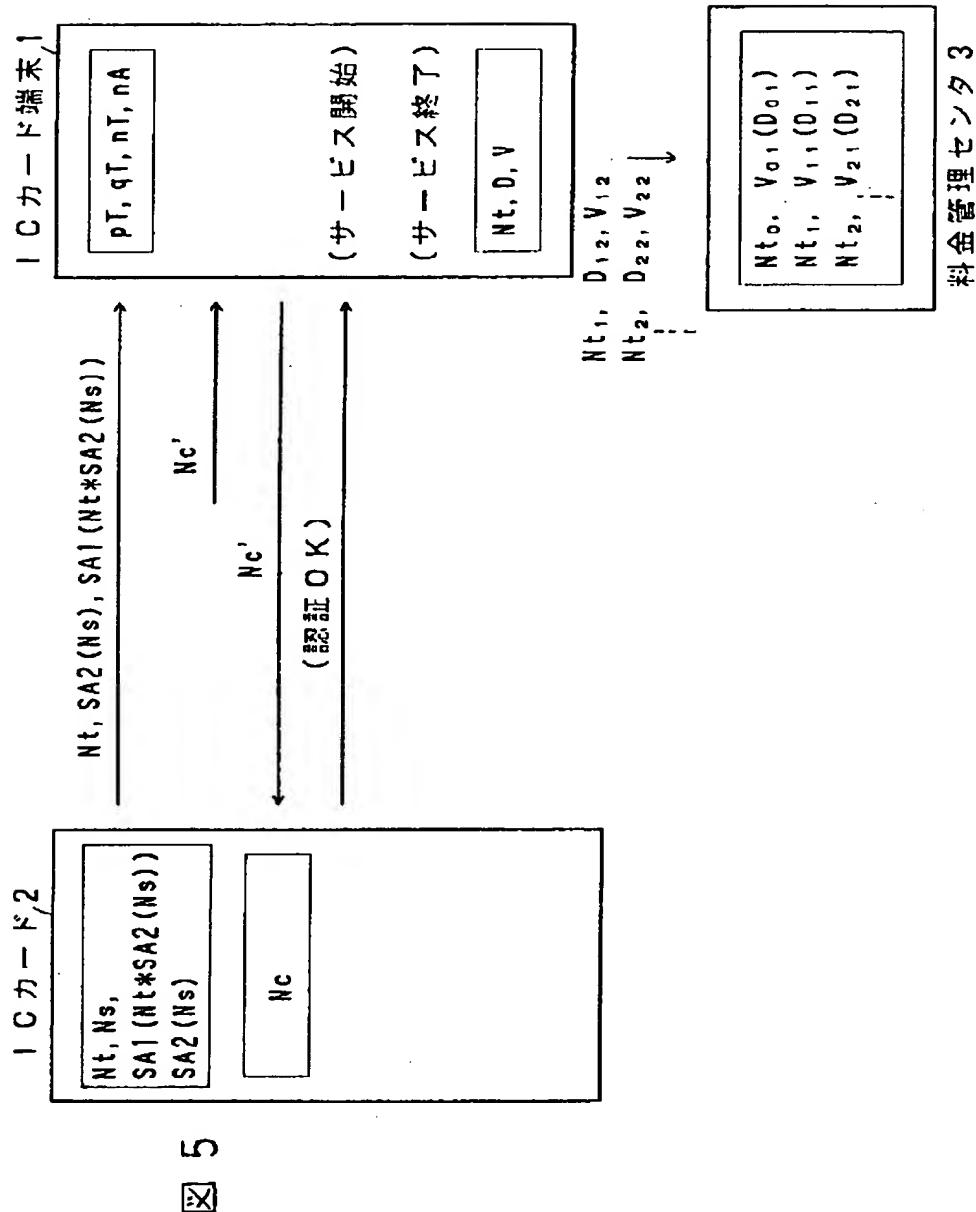
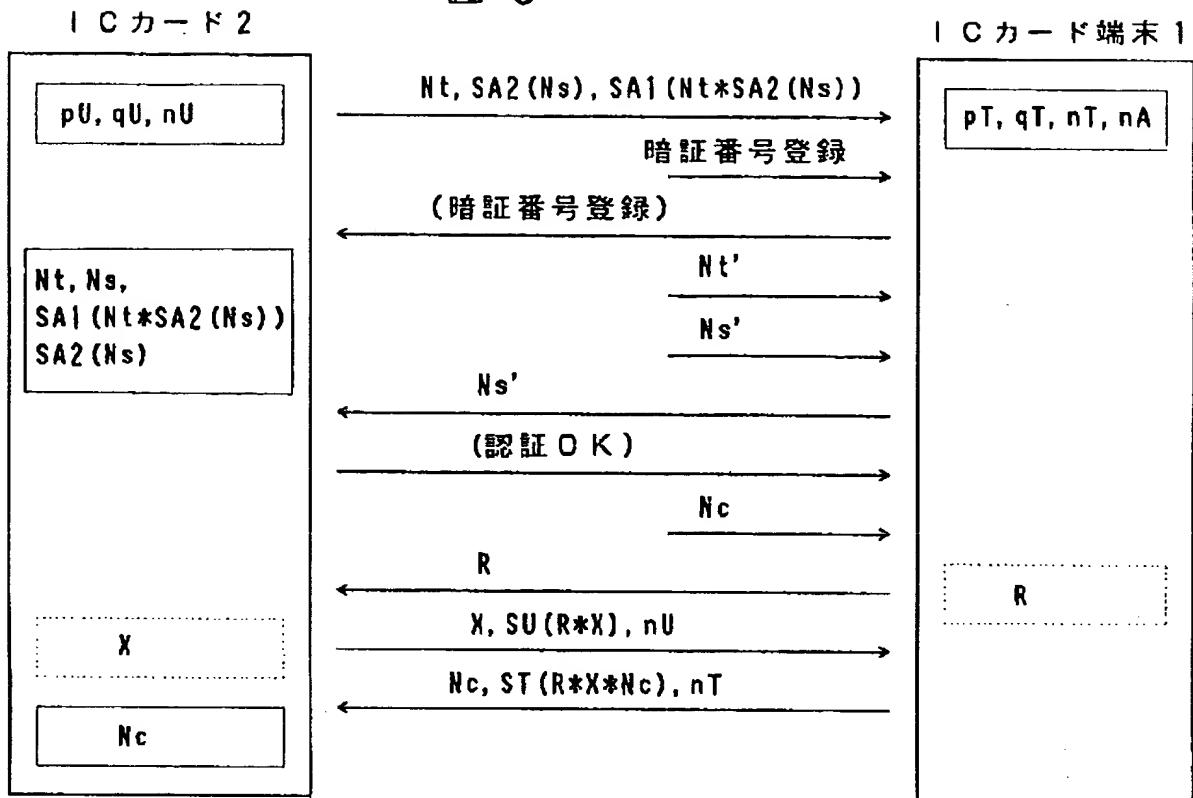


図5

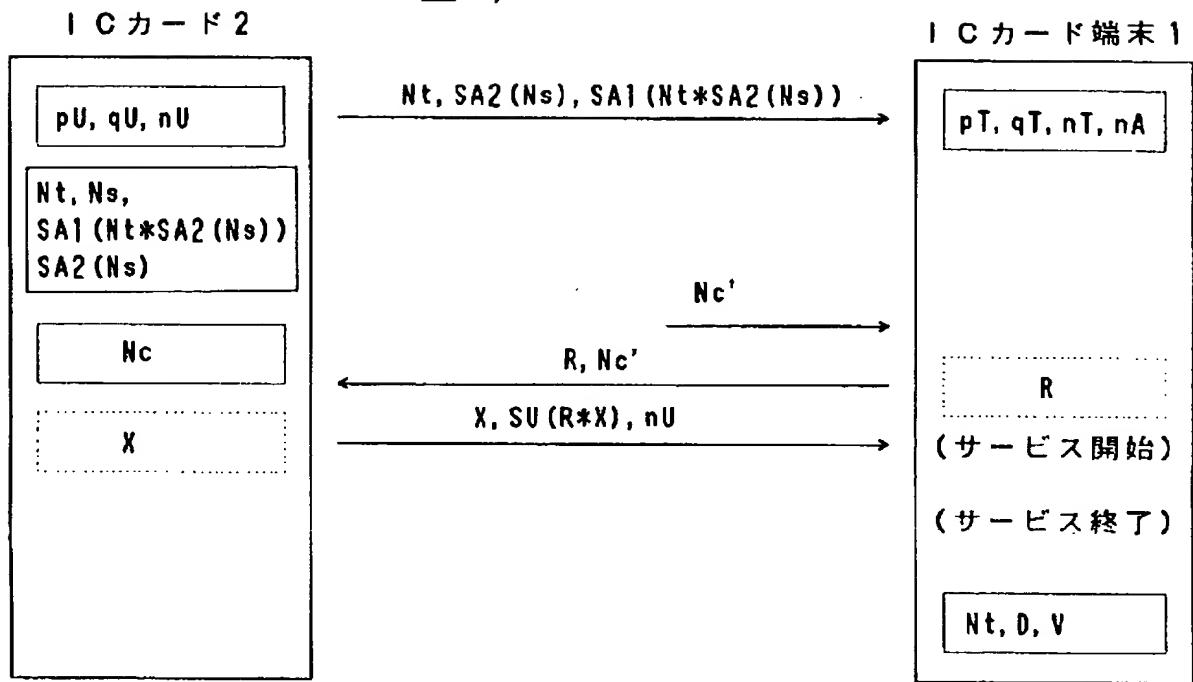
【図6】

図 6



【図7】

図 7



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**